WG#17: Optimized Authentication

Report Summary

- **Problem Description / Technical Scope**
  - Authentication is assurance of identity (computer, device, user)
  - Based on something you know (password or key), something you have (token or smartcard), something you are (fingerprint or retinal pattern), your location (terminal or longitude/latitude), time
  - Basis for other services (access control, authorization, audit, accountability)
  - Today's mechanisms are unable to satisfy needs of tomorrow's high-performance, large-scale systems

Report Summary

- **Major Technical Challenges**
  - High Performance Mechanisms
  - Very Large Scale Systems
  - Survivable Authentication Mechanisms
  - Cross-Domain Authentication
  - Dynamic Reconfiguration
  - Continuous Authentication

Addressing the Challenges

- **Challenges**
  - **C1:** High performance, optimized mechanisms
    - High speed
    - Low bandwidth
    - Optimized selection

Addressing the Challenges

- **Challenges**
  - **C2:** Very Large Scale Systems
    - Trusted Third Parties (key distribution centers, certificate authorities, on-line vs. off-line)
    - Revocation (timeliness of bindings, push vs. pull, on-line vs. off-line)
    - Common, standard interfaces

Addressing the Challenges

- **Challenges**
  - **C3:** Survivable Authentication Mechanisms
    - Reconstitution of authentication “subnets” after lose of connectivity of clocks, databases, etc., in robust manner, w/o deadlock, …
    - Recovery strategies, redundancy
    - Graceful degradation

Addressing the Challenges

- **Challenges**
  - **C4:** Cross-Domain Authentication
    - Mapping between trust models
    - Global naming
    - Formal policy representation (also local issue)
      - Strength, speed, crypto algorithm, ...
    - Single Sign-On (SSO)

Addressing the Challenges

- **Challenges**
  - **C5:** Dynamic Reconfiguration
    - Authentication module authentication
  - **C6:** Continuous Authentication
    - Firearms analogy
    - Periodic checks, pattern

Addressing the Challenges

- **Novel Approaches**
  - High performance mechanisms
  - Optimized mechanism selection
    - Strength/speed/security level tradeoff
    - Dynamic reconfiguration
  - New models and paradigms
    - Hierarchical, metricated policy model
    - Authentication “stages”

Projected Outcome

- **Success of:**
  - Active Nets
  - GloMo
  - Survivable high-confidence networks
  - Quorum
  - Adaptive computing systems
  - Collaborative technologies
  - EVERYTHING ELSE

Investment Strategy

- DARPA, Industry Support
  - Why DARPA?
  - What other collaborations?
- What if we did not do this?
- Optimal Scale of Efforts
  - small vs large? mix?

Other Issues Addressed

- **Other Challenges/Issues**
  - Interrelationship with authorization, and other security services
  - Trusted time source
  - Cold start / restart